from DOD, the systems notice will be published in the FEDERAL REGISTER for comment by the public. In the case of an exempt system of records, it will also be published at 32 CFR part 701. A listing of all DON PA systems of records notices is available at *http://www.privacy.navy.mil*.

(2) A DON activity may not begin collecting or maintaining PPI about individuals that is retrieved by their name and/or personal identifier until a PA system of records notice has been approved and published in the FEDERAL REGISTER. Failure to comply with this mandate could result in both criminal and civil penalties.

(3) In those cases where a system of records has been cancelled or deleted and it is later determined that it should be reinstated or reused, a new system notice must be prepared.

(4) DON activities wishing to create a new PA system of records must conduct a risk analysis of the proposed system to consider the sensitivity and use of the records; present and projected threats and vulnerabilities; and projected cost effectiveness of safeguards. (See § 701.118 regarding PIAs.)

(b) *Altering a system of records notice*. A systems manager shall contact CNO (DNS–36)/CMC (ARSF) to alter a PA system of records notice when there has been:

(1) A significant increase or change in the number or types of individuals about who records are maintained. For example, a decision to expand a system of records that originally covered personnel assigned to only one activity to cover personnel at several installations would constitute an altered system. An increase or decrease in the number of individuals covered due to normal growth or decrease is not an alteration.

(2) A change that expands the types or categories of information maintained.

(3) A change that alters the purpose for which the information is used. In order to be an alteration, the change must be one that is not reasonably inferred from any of the existing purposes.

(4) A change that adds a new routine use.

(5) A change to equipment configuration (either hardware or software) that creates substantially greater use of records in the system. For example, placing interactive computer terminals at regional offices when the system was formerly used only at the headquarters would be an alteration.

(6) A change in the manner in which records are organized or in the method by which records are retrieved.

(7) A combining of record systems due to reorganization.

(c) *Amending a system of records notice*. DON activities should apprise CNO (DNS–36) or CMC (ARSF) respectively when a minor change has been made to a system of records.

(d) *Deleting a system of records notice*. When a system of records is discontinued, incorporated into another system, or determined to be no longer subject to this instruction, a deletion notice must be published in the FEDERAL REGISTER. The deletion notice shall include the system identification number, system name, and the reason for deleting it. If a system is deleted through incorporation into or merger with another system, identify the successor system in the deletion notice. Systems managers who determine that a systems notice is no longer needed should contact CNO (DNS–36)/CMC (ARSF) who will prepare the deletion notice and submit it electronically to DOD for publication in the FEDERAL REGISTER.

(e) *Numbering a system of records notice*. Systems of records notices are identified with an ''N'' for a Navy system; ''M'' for a Marine Corps system; or an ''NM'' to identify a DON-wide system, followed by the subject matter Standard Subject Identification Code (SSIC).

(f) *Detailed information*. Detailed information on how to write, amend, alter, or delete a PA system of records notice is contained at *http://www.privacy.navy.mil*.

§ 701.118 Privacy, IT, and PIAs.

(a) *Development*. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and storage design. This applies to all of the development methodologies and system life cycles used in the DON.

(b) *E-Government Act of 2002.* The E-Government Act of 2002 (Pub. L. 107–347) directs agencies to conduct reviews of how privacy issues are considered when purchasing or creating new IT systems or when initiating new electronic collections of IIF. See DOD Memo of 28 Oct 05, subject ''DOD PIA Guidance'' regarding DOD PIA Guidance.

(c) *Purpose.* To ensure IIF is only acquired and maintained when necessary and the supporting IT that is being developed and used protects and preserves the privacy of the American public and to provide a means to assure compliance with applicable laws and regulations governing employee privacy. A PIA should be prepared before developing or procuring a general support system or major application that collects, maintains, or disseminates IIF from or about DON civilian or military personnel.

(d) *Scope.* The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design. During the early stages of the development of a system, both the system owner and system developer shall work together to identify, evaluate, and resolve any privacy risks. Accordingly,

(1) System owners must address what data is to be used, how the data is to be used, and who will use the data.

(2) System developers must address whether the implementation of the owner's requirements presents any threats to privacy.

(e) *Requirements.* Before developing, modifying or establishing an automated system of records that collects, maintains, and/or disseminates IIF, DON activities shall conduct a PIA to effectively address privacy factors. Guidance is provided at *http://www.doncio.navy.mil.*

(f) *Coverage.* E-Government Act of 2002 (Pub. L. 107–347) mandates the preparation of a PIA either before developing or procuring IT systems that collect, maintain, or disseminate IIF from or about members of the public or initiating a new electronic collection of IIF for 10 or more persons of the public. (NOTE: The public DOES NOT include DON civilian or military personnel, but DOES cover family members of such personnel, retirees and their family members, and DON contractors.) A PIA should be prepared before developing, modifying, or procuring IT systems that collect, maintain, or disseminate IIF from or about members of the public or initiating a new electronic collection of IIF for 10 or more members of the public. A PIA shall also be prepared before developing, modifying or procuring a general support system or major application that collects, maintains, or disseminates IIF from or about DON civilian and military personnel.

(g) *PIA not required.* (1) Legacy systems do not require completion of a PIA. However, DON CIO may request a PIA if the automation or upgrading of these systems puts the data at risk.

(2) Current operational systems do not require completion of a PIA. However, if privacy is a concern for a system the DON CIO can request that a PIA be completed. If a potential problem is identified concerning a currently operational system, the DON will use all reasonable efforts to remedy the problem.

§ 701.119 Privacy and the web.

DON activities shall consult SECNAVINST 5720.47B for guidance on what may be posted on a Navy Web site.

§ 701.120 Processing requests that cite or imply PA, Freedom of Information (FOIA), or PA/FOIA.

Individuals do not always know what Act(s) to cite when requesting information. Nonetheless, it is DON policy to ensure that they receive the maximum access to information they are requesting. Accordingly, processing guidance is as follows:

(a) *Cite/imply PA.* (1) Individuals who cite to the PA and/or seek access to records about themselves that are contained in a PA system of records that is retrieved by their name and personal identifier, will have their request processed under the provisions of the PA.

(2) If there is no ''Exemption Claimed for this System,'' then the record will be released to the requester unless: it contains classified information ((k)(1)